

(12)特許協力条約に基づいて公開された国際出願

(19)世界知的所有権機関
国際事務局



(43)国際公開日
2005年11月10日(10.11.2005)

PCT

(10)国際公開番号
WO 2005/107139 A1

(51)国際特許分類⁷:

H04L 9/08

(72)発明者;および

(21)国際出願番号:

PCT/JP2005/007894

(75)発明者/出願人(米国についてのみ):村上 隆史(MURAKAMI, Takashi).新谷 保之(SHINTANI, Yasuyuki).

(22)国際出願日:

2005年4月26日(26.04.2005)

(74)代理人:小谷 悅司, 外(KOTANI, Etsuji et al.);〒5300005大阪府大阪市北区中之島2丁目2番2号ニチメンビル2階Osaka(JP).

(25)国際出願の言語:

日本語

(81)指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD,

(26)国際公開の言語:

日本語

(30)優先権データ:

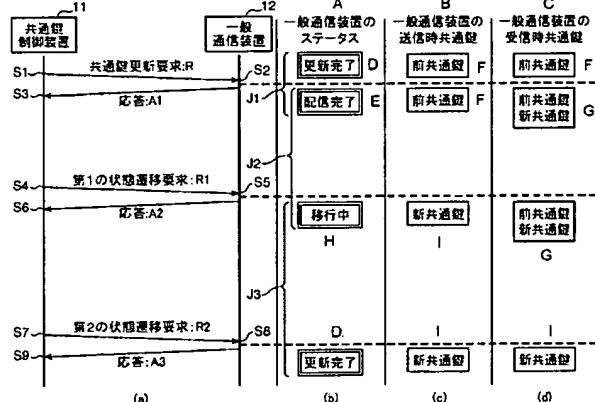
特願2004-133100 2004年4月28日(28.04.2004)JP

(71)出願人(米国を除く全ての指定国について):松下電器産業株式会社(MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.)[JP/JP];〒5718501大阪府門真市大字門真1006番地Osaka(JP).

/総葉有/

(54)Title: COMMUNICATION SYSTEM, COMMON KEY CONTROL APPARATUS, AND GENERAL COMMUNICATION APPARATUS

(54)発明の名称: 通信システム、共通鍵制御装置、及び一般通信装置



- 11... COMMON KEY CONTROL APPARATUS
R... REQUEST COMMON KEY UPDATE
A1... RESPOND
R1... REQUEST FIRST STATUS TRANSITION
A2... RESPOND
R2... REQUEST SECOND STATUS TRANSITION
A3... RESPOND
12... GENERAL COMMUNICATION APPARATUS
A... STATUS OF GENERAL COMMUNICATION APPARATUS
D... UPDATE COMPLETION
E... DISTRIBUTION COMPLETION
H... TRANSITION
B... COMMON KEY OF GENERAL COMMUNICATION APPARATUS DURING TRANSMISSION
F... PREVIOUS COMMON KEY
I... NEW COMMON KEY
C... COMMON KEY OF GENERAL COMMUNICATION APPARATUS DURING RECEPTION
G... PREVIOUS AND NEW COMMON KEYS

する際に、一般通信装置のメモリ消費量を抑制しつつ、全ての一般通信装置間で暗号化したデータを用いて相互に通

(57)要約: 共通鍵を新しい共通鍵で更新

/総葉有/

WO 2005/107139 A1

ATTACHMENT A



SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA,
UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML,
MR, NE, SN, TD, TG).

(84) 指定国(表示のない限り、全ての種類の広域保護
が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA,
SD, SL, SZ, TZ, UG, ZM, ZW), ヨーラシア (AM, AZ,
BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE,
BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU,
IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR),

添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される
各PCTガゼットの巻頭に掲載されている「コードと略語
のガイドノート」を参照。

信することができなくなる期間の発生を防止する。 共通鍵制御装置11は、全ての一般通信装置12のステータスが配信完了になったとき、全ての一般通信装置に第1の状態遷移要求R1を送信し、全ての一般通信装置12のステータスが移行中になったとき、全ての一般通信装置に第2の状態遷移要求R2を送信する。一般通信装置12は、共通鍵制御装置11から新共通鍵を受信したとき、ステータスを更新完了から前記配信完了に遷移させ、前記第1の状態遷移要求を受信したとき、ステータスを前記配信完了から前記移行中に遷移させ、前記第2の状態遷移要求を受信したとき、ステータスを前記移行中から更新完了に戻す。